Reductions of the Main Conjecture

R. Sujatha

Abstract The main goal of this article is to discuss the relevant background needed to state the noncommutative main conjecture for certain totally real p-adic Lie extensions, and to make the important reduction to the case when the Galois group of the p-adic Lie extension is of dimension one and pro-p.

Keywords K-theory • determinant • p-adic Lie groups • representations

1 Introduction

Let F be a totally real number field and p an odd prime. Fix a finite set of primes Σ of F such that Σ contains the primes above p and let F_Σ be the maximal extension of F unramified outside Σ. Suppose that F_∞/F is an abelian p-adic Lie extension of F which is totally real, contained in F_Σ, and containing the cyclotomic $\mathbb{Z}_p$-extension F^{cyc}, such that $G = \mathrm{Gal}(F_\infty/F)$ is an abelian p-adic Lie group of dimension one. Then $G \simeq H \times \Gamma$ where $\Gamma \simeq \mathbb{Z}_p$ is the Galois group of the cyclotomic $\mathbb{Z}_p$-extension F^{cyc}/F, and H is a finite abelian group. Put $\hat{H}$ for the group of 1-dimensional characters of H. Let $\mathcal{O}$ be the ring of integers of the field obtained by attaching the values of elements in $\hat{H}$ to $\mathbb{Q}_p$. Let $\Lambda_{\mathcal{O}}(G)$ be the Iwasawa algebra of G with coefficients in $\mathcal{O}$ (see Sect. 2) and write $Q_{\mathcal{O}}(G)$ for the total ring

R. Sujatha (✉)
School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai, 400 005, India

Department of Mathematics, University of British Columbia, Mathematics Road 1984, V6T 1Z2, Vancouver, BC, Canada
e-mail: sujatha@math.ubc.ca

J. Coates et al. (eds.), *Noncommutative Iwasawa Main Conjectures over Totally Real Fields*, Springer Proceedings in Mathematics & Statistics 29,
DOI 10.1007/978-3-642-32199-3_2, © Springer-Verlag Berlin Heidelberg 2013

of fractions of $\Lambda_{\mathcal{O}}(G)$. An element μ of $Q_{\mathcal{O}}(G)$ is called a *pseudomeasure* on G if $(\sigma - 1)\mu$ is in $\Lambda_{\mathcal{O}}(G)$ for all σ in G. Given a pseudomeasure μ, the integral

$$\int_G \psi \, d\mu,$$

of any nontrivial continuous homomorphism $\psi : G \to \mathcal{O}^\times$ against μ gives a well defined element of the fraction field of $\mathcal{O}$. Let κ_F denote the character which vanishes on H and restricts to the cyclotomic character on Γ. A result due to Cassou-Noguès and independently, Deligne-Ribet, asserts the existence of a unique pseudomeasure $\zeta_{F_\infty/F}$ on G such that for all χ in $\hat{H}$, we have

$$\int_G \chi \kappa_F^n d\zeta_{F_\infty/F} = L_\Sigma(\chi, 1-n), \tag{1}$$

for all integers $n > 0$ with $n \equiv 0 \bmod k$, where $k = [F(\mu_p) : F]$, μ_p denotes the group of p-th roots of unity, and $L_\Sigma(\chi, s)$ is the imprimitive complex L-function with the Euler factors corresponding to the primes in Σ being omitted in the Euler product.

For any field extension L of F, let $M(L)$ be the maximal abelian p-extension of L contained in F_Σ and let $X(L) = \mathrm{Gal}(M(L)/L)$. Now let K be any finite extension of $\mathbb{Q}$ (K need not be totally real). The classical Iwasawa $\mu = 0$ conjecture for K and the prime p is the assertion that, the Galois group over K^{cyc} of the maximal unramified abelian p-extension of K^{cyc} is a finitely generated $\mathbb{Z}_p$-module. This is known to be true for all abelian extensions K of $\mathbb{Q}$ and all primes p, thanks to work of Ferrero-Washington. Moreover, a well-known argument in Kummer theory shows that if F is any totally real field and $K = F(\mu_p)$, then the validity of the classical Iwasawa conjecture (see [CK, Sect. 3]) for K implies that $X(F^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module. The aim of the abelian main conjecture is to give a precise relation between the analytic pseudomeasure $\zeta_{F_\infty/F}$ and the algebraic structure of the $\Lambda_{\mathcal{O}}(G)$-module $X(F_\infty)$. The precise assertion is discussed in the article by Coates and Kim [CK] in this volume. As is explained there, stating the assertion of the main conjecture is delicate even in this classical case, when H has order divisible by p. The reader is referred to *loc.cit.* for a careful discussion leading to the assertion of the main conjecture, which is a fundamental theorem due to Wiles [Wi].

The goal then is to first formulate an analogue of the main conjecture for field extensions F_∞/F that are admissible, (see [CK, Sect. 1] for the precise definition) totally real p-adic Lie extensions of F, and prove the conjecture in some special cases. As in [CK, Sect. 3], the extension F_∞/F is said to satisfy *Iwasawa Conjecture* if there exists a finite extension F' of F in F_∞ such that $\mathrm{Gal}(F_\infty/F')$ is pro-p, and $X(F'^{\mathrm{cyc}})$ is a finitely generated $\mathbb{Z}_p$-module. In our present state of knowledge, we can prove this main conjecture only when the Iwasawa conjecture holds (see [CK, Sect. 3]) for F_∞. Let $G = \mathrm{Gal}(F_\infty/F)$ and $\Lambda(G)$ be the corresponding Iwasawa algebra, which is a Noetherian noncommutative ring. Then

$X(F_\infty)$ is a finitely generated module over $\Lambda(G)$. The philosophy of the main conjecture is to relate an algebraic invariant (the *'characteristic element' of* $X(F_\infty)$) to an analytic invariant, (namely the *'p-adic L-function'*) that interpolates values of the complex L-function. These should be viewed as the counterparts of the characteristic element and the pseudomeasure discussed earlier in the abelian case. However, in the nonabelian case, these invariants lie in the K_1 group of a certain noncommutative localization of the Iwasawa algebra $\Lambda(G)$. A precise formulation of the noncommutative main conjecture, and its proof due to M. Kakde was the goal of the series of lectures given at the workshop. The reader is referred to [CK, Sect. 5] and Sect. 2 below for a fuller discussion of this theme. In this introduction, we only point out that even for formulating the main conjecture in this context, it is necessary to assume the analogue of Iwasawa's $\mu = 0$ conjecture (see [CK, Sect. 1]), which is equivalent here to assuming that $X(F_\infty)$ is finitely generated as a $\Lambda(H)$-module where $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. Further, in this nonabelian context, the analogue of (1) involves a formulation in terms of noncommutative determinants using K-groups and Euler characteristics.

The main aim of this article is to formulate the noncommutative main conjecture, and to discuss the reduction of its proof for totally real fields to the case when the p-adic Lie extension F_∞/F has dimension one, with pro-p Galois group G. An intermediate important step is to consider the case when G is isomorphic to $\Delta \times G_p$, where G_p is a compact pro-p, p-adic Lie group of dimension one and Δ is a finite group of order prime to p. We stress that in the general nonabelian case, the hypothesis that $X(F_\infty)$ satisfies the analogue of Iwasawa's $\mu = 0$ conjecture is necessary both for the formulation of the main conjecture and in its proof. That such a reduction to the one dimensional case is possible, was first proved by Burns [Bu]. When Δ is abelian, this reduces to the classical abelian case where the main conjecture is known, thanks to the result of Wiles, and is dealt with in [CK]. In the general case, Kakde's proof then proceeds by a delicate study of the K_1-group of the relevant localization of the Iwasawa algebra $\Lambda(G)$ and forms the technical core of the proof. This is the subject of the article by Schneider and Venjakob [SV] in this volume. These algebraic results serve as a crucial step in reducing the proof to verifying certain congruence relations between the Deligne-Ribet, Cassou-Nogués p-adic zeta functions for abelian one dimensional extensions, and this forms the basis of constructing the desired p-adic L-function. This step uses the analogue of the $\mu = 0$ hypothesis, i.e. that $X(F'_\infty/F)$ is a finitely generated $\mathbb{Z}_p$-module, where F'_∞ is the extension of F corresponding to the fixed field of F_∞ by the subgroup G_p, and rests on a strategy of Burns and Kato. The final step of verifying the required congruences is executed using the Deligne-Ribet q-expansion principle.

Here is the plan of the article. As the general formulation of the noncommutative main conjecture needs the localization sequence in algebraic K-theory, we will begin by providing a quick review of the K-groups K_0 and K_1 and also the relevant localization exact sequence in Sect. 1. In Sect. 2, we discuss the necessary background that is needed and then state the noncommutative conjecture. For the proofs of the results stated, the reader is referred to [B] or [Sw]. Finally, in Sect. 3, we show how the proof of the main conjecture can be reduced to the case of a special one dimensional p-adic Lie extension, following the arguments of Kakde. The reader is strongly encouraged to consult the papers of Ritter and Weiss (especially [RW]) for another approach of the proof of the main conjecture. We mention that Venjakob's article [V1] in this volume compares Kakde's proof with that of Ritter and Weiss. *Throughout these notes, all rings considered will be (not necessarily commutative) unital, associative, left and right Noetherian rings, and modules shall mean left modules.* Finally, the author is grateful to John Coates and the referee for their comments that helped improve the exposition of the article.

2 Algebraic K-Theory

Let $\mathcal{C}$ be an abelian category. Recall that a nonempty full subcategory $\mathcal{D}$ of $\mathcal{C}$ is a *Serre subcategory* if given an exact sequence

$$A' \xrightarrow{f} A \xrightarrow{g} A''$$

in $\mathcal{C}$, we have that A' and A'' are objects in $\mathcal{D}$ if and only if A is an object in $\mathcal{D}$. The group $K_0(\mathcal{C})$ is the abelian group generated by classes $[A]$, where A runs over the objects of $\mathcal{C}$, and subject to the relation

$$[A] = [A'] + [A''],$$

for each short exact sequence

$$0 \to A' \to A \to A'' \to 0$$

in $\mathcal{C}$. The group $K_0(\mathcal{C})$ is universal with respect to this property in the following sense. Suppose we are given an abelian group G and a map $f : \mathrm{Ob}(\mathcal{C}) \to G$, such that for each short exact sequence

$$0 \to A' \to A \to A'' \to 0$$

in $\mathcal{C}$, we have $f(A) = f(A') + f(A'')$ in G. Then there exists a unique homomorphism $\phi : K_0(\mathcal{C}) \to G$ making the diagram

$$\begin{tikzcd} \mathrm{Ob}(\mathcal{C}) \arrow[rr] \arrow[dr, "f"'] & & K_0(\mathcal{C}) \arrow[dl, "\phi"] \\ & G & \end{tikzcd}$$

commutative. More generally, the group K_0 can be defined analogously for any *exact category*, which we will not define rigorously (see [B]); intuitively, it is an additive category in which exact sequences are well-defined. Then the map

$$\mathcal{C} \to K_0(\mathcal{C})$$

is a covariant functor from the category of abelian categories and exact functors to Ab, the category of abelian groups. The following proposition is well-known.

Proposition 2.1. *Let A, B be objects of $\mathcal{C}$. If $[A] = [B]$ in $K_0(\mathcal{C})$, then there is an object $C \in \mathcal{C}$ such that $A \oplus C \simeq B \oplus C$.*

Examples:

(i) Let k be a field and $\mathcal{C}$ be the category of finite dimensional vector spaces. Then $K_0(\mathcal{C}) \simeq \mathbb{Z}$, the isomorphism being given by the dimension homomorphism.
(ii) Let $\mathcal{C}$ be the category of finite abelian groups. Then $K_0(\mathcal{C})$ is free abelian on the basis $[\mathbb{Z}/p\mathbb{Z}]$, where p runs over all primes. This is seen to be true via an induction argument on the cardinality of the finite group, combined with the structure theorem for finite abelian groups. The statement also follows from the Jordan-Hölder theorem along with the fact that a simple abelian group has the form $\mathbb{Z}/p\mathbb{Z}$ for some prime p.
(iii) Let R be a ring and $\mathcal{C}_R$ be the category of finitely generated (left) R-modules and let $\mathcal{P}_R$ be the full subcategory of $\mathcal{C}_R$ consisting of finitely generated projective left R-modules. This is an exact category, and the natural inclusion $\mathcal{P}_R \subset \mathcal{C}_R$ induces a homomorphism $K_0(\mathcal{P}_R) \to K_0(\mathcal{C}_R)$.

Definition 2.1. Let R be a ring. The group $K_0(R)$ is defined to be the group $K_0(\mathcal{P}_R)$.

Proposition 2.2 (see [Sw, Part II, Chap. 1]). *Let R be a ring. Then the following assertions hold:*

(i) The group $K_0(\mathcal{P}_R)$ is generated by $[P]$, where P is a finitely generated projective R-module with the relations $[P] = [Q]$ if $P \simeq Q$ and $[P \oplus Q] = [P] + [Q]$.
(ii) Any element of $K_0(R)$ can be written as $[P] - [Q]$ for finitely generated projective R-modules P and Q. Further, $[P] - [Q] = [P'] - [Q']$ in $K_0(R)$ if and only if there is a finitely generated projective R-module M such that $P \oplus Q' \oplus M = P' \oplus Q \oplus M$.

Given a ring homomorphism $\eta : R \to R'$, the base change map $P \mapsto R' \otimes_R P$ induces a group homomorphism $K_0(R) \to K_0(R')$ as η induces an exact functor from the category $\mathcal{P}_R$ to $\mathcal{P}_{R'}$. We shall also need the following result (see [Sw, Part II, Chap. 2, Proposition 2.29]).

Proposition 2.3. *If R is complete with respect to a two sided ideal I, the map $K_0(R) \to K_0(R/I)$ induced by the projection $R \to R/I$ is an isomorphism.*

The following result due to A. Heller, is important in relating $K_0(R)$ and $K_0(\mathcal{C}_R)$. Recall that a subcategory $\mathcal{A}$ is *closed under subobjects (resp. quotient objects) in $\mathcal{C}$* if subobjects (resp. quotient objects) in $\mathcal{C}$ of an object in $\mathcal{A}$ are again in $\mathcal{A}$.

Theorem 2.1 ([Sw, Part II, Chap. 3, Theorem 3.1]). *Let $\mathcal{C}$ be an abelian category, $\mathcal{A}$ and $\mathcal{B}$ be full subcategories with $\mathcal{A} \subset \mathcal{B}$, and such that $\mathcal{A}$ is closed in $\mathcal{C}$ under* *subobjects and quotient objects. Assume further that every object of $\mathcal{B}$ has a finite filtration with all quotients in $\mathcal{A}$. Then the canonical map $K_0(\mathcal{A}) \to K_0(\mathcal{B})$ is an isomorphism.*

Definition 2.2. For a ring R, the group $G_0(R)$ is defined to be the abelian group $K_0(\mathcal{C}_R)$.

Note that the inclusion $\mathcal{P}_R \subset \mathcal{C}_R$ induces a group homomorphism (see *loc.cit.* Corollary 4.6)

$$i : K_0(R) \to G_0(R), \tag{2}$$

called the *Cartan homomorphism*.

Theorem 2.2 ([Sw, Part II, Chap. 3, Proposition 3.4]). *Let I be a nilpotent two sided ideal of a ring R. Then the map $G_0(R/I) \to G_0(R)$ given by $[A] \mapsto [A]$ is an isomorphism.*

Suppose that $h : R \to R'$ is a ring homomorphism such that R' is flat as an R-module. Then the natural functor $\mathcal{C}_R \to \mathcal{C}_{R'}$ obtained from the base change map induces a homomorphism $G_0(R) \to G_0(R')$. To make precise the relationship between $G_0(R)$ and $K_0(R)$, we need some more groundwork.

Definition 2.3. Let $\mathcal{C}$ be an abelian category. Recall that an object $P \in \mathcal{C}$ is *projective* if the functor

$$\mathrm{Hom}\,(P,\ ) : \mathcal{C} \to \mathrm{Set}$$

preserves epimorphisms. The *projective dimension* of $A \in \mathrm{Ob}(\mathcal{C})$ denoted $\mathrm{pd}(A)$ is the smallest n such that there exists an exact sequence

$$0 \to P_n \to P_{n-1} \to \cdots P_0 \to A \to 0$$

with all the P_i's projective. If the projective dimension of A is undefined we write $\mathrm{pd}(A) = \infty$. In the particular case that $\mathcal{C} = \mathcal{C}_R$, we say that R has *finite global dimension* $\leq n$ if every object of $\mathcal{C}_R$ has finite projective dimension at most n.

Commutative regular local rings have finite global dimension n where n is the Krull dimension of R. This is a deep result of Auslander-Buchsbaum in commutative ring theory. In noncommutative ring theory, Noetherian Auslander regular local rings [Bj] are known to have finite global dimension. For such rings, there is a well developed dimension theory for modules which plays a central role.

Theorem 2.3 ([Sw, Theorem 4.4]). *Let $\mathcal{C}$ be an abelian category and $\mathcal{P}$ be the full subcategory of projective objects. If* $\mathrm{pd}(A) < \infty$ *for every A in $\mathcal{C}$, then the natural map $K_0(\mathcal{P}) \to K_0(\mathcal{A})$ is an isomorphism. In particular, if a ring R has finite global dimension, then the natural homomorphism $i : K_0(R) \to G_0(R)$ is an isomorphism.*

Corollary 2.1 (cf. [Sw, Corollary 4.6]). *Let R be a commutative Noetherian regular local ring or a noncommutative Noetherian Auslander regular local ring. Then the natural homomorphism $i : K_0(R) \to G_0(R)$ is an isomorphism.*

If $\mathcal{C}$ is an abelian category, $\mathcal{P}$ is the full subcategory of projective objects, and $\mathcal{H}$ the full subcategory of all $A \in \mathcal{C}$ with $\mathrm{pd}A < \infty$ (note that $\mathcal{H}$ need not be an abelian category, but it is an exact category), then the natural map $K_0(\mathcal{P}) \to K_0(\mathcal{H})$ is again an isomorphism. If $\mathcal{B}$ is a full, exact subcategory such that $\mathcal{P} \subset \mathcal{B} \subset \mathcal{H}$, then the natural map $K_0(\mathcal{P}) \to K_0(\mathcal{B})$ is a split mono. It is onto if for every exact sequence $0 \to C \to P \to B \to 0$, $P \in \mathcal{P}$ and $B \in \mathcal{B}$ implies $C \in \mathcal{B}$.

We next deal with localization and the corresponding maps between G_0 (see [Sw, Chap. 5]). Let R be a ring and S a subset such that S contains 1 and is either a multiplicatively closed set contained in the centre of R or a left and right Ore set. *For ease of exposition, we shall always assume that the elements of S are not zero divisors in R*. In both these cases, the corresponding localizations exist and we denote by R_S the localized ring. For a module M over R, the localization is denoted by M_S. The natural map $f : M \to M_S$ given by $f(m) = m/1$ is an R-homomorphism and a ring homomorphism in the special case when $M = R$. The kernel $\mathrm{Ker}\,(f)$ consists of the set of elements $m \in M$ such that there exists an element $s \in S$ with $sm = 0$. Recall that R_S is a flat R-module. Let $\mathcal{C}_S$ be the subcategory consisting of finitely generated R-modules M such that $M_S = 0$. Then $\mathcal{C}_S$ is a Serre subcategory and there is an exact sequence (*loc.cit.* Corollary 5.14)

$$K_0(\mathcal{C}_S) \to K_0(R) \to K_0(R_S). \tag{3}$$

The right map is not always surjective, but there is always an exact sequence

$$K_0(\mathcal{C}_S) \to G_0(R) \to G_0(R_S) \to 0. \tag{4}$$

If the ring R (and hence the ring R_S) has finite global dimension, then (3) gives an exact sequence

$$K_0(\mathcal{C}_S) \to K_0(R) \to K_0(R_S) \to 0. \tag{5}$$

To deal with a broader class of rings which do not necessarily have finite global dimension, and also to extend the above exact sequences on the left with K_1 groups, we introduce the notion of the *relative K-group*. For more details, the reader is referred to Weibel's book [We].

Definition 2.4. Let $f : R \to R'$ be a ring homomorphism. The category C_f consists of triplets (P, a, Q) as objects, where P and Q are finitely generated projective R-modules, and a is an isomorphism

$$a : R' \otimes_R P \xrightarrow{a} R' \otimes_R Q.$$

Morphisms between two objects (P, a, Q) and (P', a', Q') consist of a pair of R-morphisms $g : P \to P'$ and $h : Q \to Q'$ such that

$$a' \circ (1_{R'} \otimes g) = (1_{R'} \otimes h) \circ a.$$

It is an isomorphism if both g and h are isomorphisms. A sequence of morphisms in C_f (see [Sw, Part II, Chap. 13])

$$0 \to (P', a', Q') \to (P, a, Q) \to (P'', a'', Q'') \to 0 \qquad (6)$$

is a short exact sequence if the underlying sequences

$$0 \to P' \to P \to P'' \to 0, \qquad 0 \to Q' \to Q \to Q'' \to 0$$

are short exact. The group $K_0(f)$ (also called the relative K_0) is an abelian group defined by generators $[(P, a, Q)]$ with (P, a, Q) an object in the category C_f subject to the following relations:

- $[(P, a, Q)] = [(P', a', Q')]$ if the two objects are isomorphic.
- $[(P, a, Q)] = [(P', a', Q')] + [(P'', a'', Q'')]$ for every short exact sequence as in (6).
- $[(P_1, b \circ a, P_3)] = [(P_1, a, P_2)] + [(P_2, b, P_3)]$.

For the natural map $\iota : R \to R_S$, the relative K-group $K_0(\iota)$ is usually denoted by $K_0(R, R_S)$. This group can also be identified with the following group. Let $\mathcal{C}_S^{hb}$ denote the category of bounded complexes of finitely generated projective R-modules whose homology modules are S-torsion. The abelian group $K_0(\mathcal{C}_S^{hb})$ is defined as the abelian group with generators $[C]$, where C is in $\mathcal{C}_S^{hb}$, and relations (1) $[C] = 0$ if the complex C is acyclic, and (2) $[C] = [C'] + [C'']$, for every short exact sequence of complexes

$$0 \to C' \to C \to C'' \to 0$$

in $\mathcal{C}_S^{hb}$. Let $\mathcal{H}_S$ denote the category of finitely generated R-modules which are S-torsion and which have a finite resolution by finitely generated projective R-modules. There are isomorphisms

$$K_0(\mathcal{C}_S^{hb}) \xleftarrow{\sim} K_0(R, R_S) \xrightarrow{\sim} K_0(\mathcal{H}_S). \qquad (7)$$

To describe the isomorphisms in the special case when S is central, first note that every isomorphism a from $R_S \otimes_R P$ to $R_S \otimes_R Q$ is of the form $s^{-1}\alpha$, where α is an R-map from P to Q and $s \in S$. The first isomorphism is given by

$$[(P, a, Q)] \mapsto [P \xrightarrow{\alpha} Q] - [Q \xrightarrow{s} Q],$$

while the second is given by

$$[(P, a, Q)] \mapsto [Q/\alpha(P)] - [Q/sQ].$$

For more general localizing sets S, the isomorphisms are a little more subtle and proceed via the *Euler characteristic*.

Definition 2.5. Given a bounded chain complex

$$C_\bullet : \ 0 \to C_m \to \cdots \to C_0 \to 0$$

of objects in an abelian category $\mathcal{C}$., the *Euler characteristic* $\chi(C_\bullet)$ of $C_\bullet$ is defined to be the element $\Sigma(-1)^i[C_i]$ of $K_0(\mathcal{C})$.

If $C_\bullet$ is a bounded complex of objects in $\mathcal{C}$, the element $\chi(C_\bullet)$ depends only upon the homology of $C_\bullet$ and $\chi(C_\bullet) = \Sigma(-1)^i[H_i(C_\bullet)]$. In particular, if $C_\bullet$ is acyclic, then $\chi(C_\bullet) = 0$. In the general case, the isomorphisms in (7) are fleshed out using the Euler characteristic map. The first isomorphism takes $[(P, a, Q)]$ to the complex $[0 \to P \xrightarrow{a} Q \to 0]$ while the second maps $[(P, a, Q)]$ to $[\mathrm{Coker}\,(a)] - [\mathrm{Ker}\,(a)]$.

We now discuss the group $K_1(R)$ for a ring R. There are various (equivalent) definitions though checking the equivalence involves several technicalities and is hence beyond the scope of these lectures. We shall largely consider the algebraic definitions which only use linear algebra and elementary group theory. Let $\mathrm{GL}_n(R)$ denote the group of $(n \times n)$ matrices over R that are invertible. Each such matrix g is naturally viewed as an $(n+1) \times (n+1)$ matrix given by $\begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix}$ and thus gives an embedding of $\mathrm{GL}_n(R)$ into $\mathrm{GL}_{n+1}(R)$. The group $\mathrm{GL}(R)$ is defined as the union

$$\bigcup_n \mathrm{GL}_n(R),$$

and is called the *infinite linear group* over R.

Recall the commutator subgroup $[G, G]$ of a group G, which is always a normal subgroup of G and is universal with respect to the quotient group being abelian. The first definition of $K_1(R)$ (also called the *Whitehead group of* R) is as the quotient of $\mathrm{GL}(R)$ by its commutator subgroup.

Definition 2.6. $K_1(R)$ is the abelian group $\mathrm{GL}(R)/[\mathrm{GL}(R), \mathrm{GL}(R)]$.

The abelian group $K_1(R)$ thus has the universal property that every homomorphism from $\mathrm{GL}(R)$ to an abelian group must factor through $K_1(R)$. Given a ring homomorphism $R \to R'$, it induces a homomorphism from $K_1(R)$ to $K_1(R')$ and K_1 is thus a covariant functor from the category of rings to Ab.

Example: If R happens to be commutative, then the determinant homomorphism is a group homomorphism from $\mathrm{GL}(R)$ onto the (abelian) group $R^\times$ of units in R, and we denote the induced surjective map from $K_1(R)$ by det,

$$\det \, : \, K_1(R) \to R^\times,$$

and the kernel of this surjection is defined to be the abelian group $\mathrm{SK}_1(R)$. There is a direct sum decomposition $K_1(R) \simeq R^\times \oplus \mathrm{SK}_1(R)$.

Recall that for an element r in R, the *elementary matrix* $e_{ij}(r)$ in $\mathrm{GL}(R)$ is the matrix which has 1 across the diagonal, r at the (i, j)-spot, and zero elsewhere.

If $\mathrm{E}_n(R)$ is the subgroup of $\mathrm{GL}_n(R)$ generated by all elementary matrices $e_{ij}(r)$ with $1 \le i, j \le n,\ i \ne j$, then the group $\mathrm{E}(R)$ is the union $\bigcup_n \mathrm{E}_n(R)$. The classical Whitehead's lemma asserts that the group $\mathrm{E}(R)$ is the commutator subgroup and therefore

$$K_1(R) \simeq \mathrm{GL}(R)/\mathrm{E}(R).$$

The group $K_1(R)$ measures the obstruction to taking an arbitrary invertible matrix over R and reducing it to the identity via a series of elementary operations.

Recall that a ring R is said to be *semilocal* if $R/\mathrm{rad}R$ is a left artinian ring, or equivalently $R/\mathrm{rad}R$ is a semisimple ring; here $\mathrm{rad}R$ is the radical of the ring R. If R has finitely many maximal left ideals, then R is semilocal. The following result of Vaserstein is very useful.

Proposition 2.4. *Let R be a semilocal ring. Then the natural inclusion of $R^\times = \mathrm{GL}_1(R)$ into $\mathrm{GL}(R)$ induces an isomorphism $K_1(R) \simeq R^\times/[R^\times, R^\times]$.*

Example:

(i) If R is the group ring $\mathbb{Z}[G]$ of a group G, the (first) Whitehead group $\mathrm{Wh}(G)$ is the quotient of $K_1(\mathbb{Z}[G])$ by the subgroup generated by ± 1 and the elements of G, considered as elements of $R^\times$ and hence in $\mathrm{GL}_1(R)$. If G is abelian, then $\mathbb{Z}[G]$ is commutative and we have

$$\mathrm{Wh}(G) = \big(\mathbb{Z}[G]^\times / \pm G\big) \oplus \mathrm{SK}_1(\mathbb{Z}[G]).$$

If G is finite, then $\mathrm{Wh}(G)$ is known to be a finitely generated group. In fact, it is known that rank $K_1(\mathbb{Z}[G])$= rank $\mathrm{Wh}(G)$, and hence $SK_1(\mathbb{Z}[G])$ is the full torsion subgroup of $K_1(\mathbb{Z}[G])$ and is in fact equal to the kernel of the natural map $K_1(\mathbb{Z}[G]) \to K_1(\mathbb{Q}[G])$.

(ii) More generally if A is a Dedekind domain with quotient field K, and G is a finite group, the group $\mathrm{SK}_1(A[G])$ is defined by

$$\mathrm{SK}_1(A[G]) = \mathrm{Ker}\,(K_1(A[G]) \to K_1(K[G])). \tag{8}$$

The important results proved by Wall, Oliver and others will be used subsequently and [O] is a good reference for this. The group $\mathrm{SK}_1(\mathbb{Z}[G])$ has interesting topological applications.

Let us now turn to an alternative definition of $K_1(R)$ using projective modules. Let P be a finitely generated projective R-module. Choosing an isomorphism $P \oplus Q \simeq R^n$ gives a group homomorphism from $\mathrm{Aut}(P)$ to $\mathrm{GL}_n(R)$, by sending α to $\alpha \oplus 1_Q$. This homomorphism is well-defined when viewed as a homomorphism into $\mathrm{GL}_n(R)$, up to inner automorphisms of $\mathrm{GL}_n(R)$, and thus there is a well-defined homomorphism $\mathrm{Aut}(P) \to K_1(R)$.

Definition 2.7. For a ring R, the group $K_1(R)$ is an abelian group which consists of generators $[P, a]$ where P is a finitely generated projective R-module and a is in $\mathrm{Aut}(P)$, subject to the relations

- $[P, a] = [Q, b]$ if there is an isomorphism $f : P \to Q$ such that $f \circ a = b \circ f$,
- $[P,\ a \circ b] = [P, a][P, b]$
- $[P \oplus Q, a \oplus b] = [P, a][Q, b]$.

The equivalence of this definition with the earlier one is seen using the well-defined homorphism from $\mathrm{Aut}(P)$ to $\mathrm{GL}(R)$ as discussed above. There is a homological interpretation of $K_1(R)$ given by

$$K_1(R) = H_1(\mathrm{GL}(R), \mathbb{Z}),$$

the first group homology of $\mathrm{GL}(R)$ with $\mathbb{Z}$-coefficients, (see [Mi]). A further topological interpretation elucidates $K_1(R)$ as $\pi_1(K(R))$ where $K(R)$ is a certain topological space built using the category $\mathcal{P}_R$.

Let R be a ring and S a (left and right) localising Ore set as before. Consider the relative K-group $K_0(R, R_S)$. There is a *connecting homomorphism*

$$\partial\ :\ K_1(R_S) \to K_0(R, R_S) \tag{9}$$

that maps an element $[P_S, \alpha_S]$ in $K_1(R_S)$ (P_S is a finitely generated projective module over R_S and α_S is an automorphism of P_S) to $[R^n, \tilde{\alpha}, R^n]$. Here P is a projective module such that $R_S \otimes_R P = P_S$ and Q is a projective R-module such that $P \oplus Q \simeq R^n$, and $\tilde{\alpha}$ is an endomorphism of R^n such that $1_{R_S} \otimes_R (\alpha \oplus 1_Q) \simeq \alpha_S$. We can also use the isomorphism of $K_1(R)$ with $\mathrm{GL}(R)/E(R)$ to define this homomorphism. Map an element g in $\mathrm{GL}(n, R)$ to $[(R^n, g, R^n)]$ in $K_0(R, R_S)$. This commutes with the map $\mathrm{GL}(n, R) \to \mathrm{GL}(n + 1, R)$ and thus gives a well-defined homomorphism from $\mathrm{GL}(R)$ to $K_0(R, R_S)$. But the latter group being abelian, this homomorphism factors to give the desired map from $K_1(R)$. There is also a homomorphism

$$\eta\ :\ K_0(R, R_S) \to K_0(R) \tag{10}$$

that maps $[(P, a, Q)]$ to $[P] - [Q]$ in $K_0(R)$. These maps are used to construct a long exact sequence of K-groups as in the theorem stated below. A proof of this theorem when S is a central multiplicatively closed set can be found in [Sw, Part II, Chap. 15].

Theorem 2.4. *Let R be a ring and S a left and right Ore set of R whose elements are nonzero divisors. Then there is an exact localization sequence*

$$K_1(R) \to K_1(R_S) \xrightarrow{\partial} K_0(R, R_S) \xrightarrow{\eta} K_0(R) \to K_0(R_S). \tag{11}$$

The sequence is surjective on the right if $K_0(R_S)$ is replaced by $G_0(R_S)$, and the same holds if the ring R has finite global dimension.

Another important property of the groups K_0 and K_1 is *Morita invariance*. If R is a ring, then this property states that there are natural isomorphisms $K_i(R) \simeq K_i(\mathrm{M}_n(R))$ for $i = 0, 1$. We shall need the *norm* or transfer maps defined in K-theory, which we recall for the K_1-groups.

Definition 2.8. Let R be a ring and R' a ring containing R such that R' is finitely generated and projective as an R-module. Let $\mathcal{P}_{R'}$ and $\mathcal{P}_R$ denote the categories of finitely generated projective modules over R' and R respectively. Then the natural forgetful functor $\mathcal{P}_{R'} \to \mathcal{P}_R$ induces a homomorphism $K_1(R') \to K_1(R)$ which is called the *norm* or *transfer* homomorphism.

A particular case of this will be that of group rings, with G a subgroup of finite index in another group G', $R' = \mathbb{Z}[G']$ and $R = \mathbb{Z}[G]$.

We shall close this section with the following definition which will be extended later to Iwasawa algebras.

Definition 2.9. Let G be a finite group and A be a Dedekind domain. Consider the group ring $R = A[G]$. The group $K_1'(A)$ is defined by $K_1'(R) = K_1(R)/\mathrm{SK}_1(R)$, where $\mathrm{SK}_1(R)$ is defined as in (8).

Finally, we remark that the integral logarithm which will be discussed in the lectures of [SV] gives a nice description of $K_1'(R)$.

3 The Noncommutative Main Conjecture

In this section, we shall formulate the Noncommutative Main Conjecture for the trivial motive over totally real fields. We shall follow notation as in the lectures of J. Coates [CK]. Thus F will denote a totally real number field and F_∞ will be an admissible, totally real p-adic Lie extension of F. An extension F_∞/F as above is said to be *admissible* if (1) the Galois group $\mathrm{Gal}(F_\infty/F)$ is a p-adic Lie group, (2) F_∞/F is unramified outside a finite set of primes Σ of F containing the primes lying above p, and (3) F_∞ contains the cyclotomic $\mathbb{Z}_p$-extension F^{cyc}. We shall further assume that the Iwasawa conjecture holds for the admissible extension F_∞. Put $G = \mathrm{Gal}(F_\infty/F)$, $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$, and let $\Lambda(G)$ denote the Iwasawa algebra

$$\Lambda(G) := \varprojlim \mathbb{Z}_p[G/U]$$

where U varies over open normal subgroups of G and the inverse limit is taken with respect to the natural surjections. If $\mathcal{O}$ is the ring of integers in a finite extension of $\mathbb{Q}_p$, then $\Lambda_{\mathcal{O}}(G)$ is the Iwasawa algebra of G over $\mathcal{O}$, defined as above with $\mathcal{O}$ replacing $\mathbb{Z}_p$. Fix a finite set Σ of primes of F that contain the primes above p, and denote the maximal extension of F that is unramified outside Σ by F_Σ. Recall that for any extension L of F contained in F_Σ, $X(L)$ is the Galois group of the maximal abelian p-extension contained in F_Σ. As discussed in the lectures by Coates, $X(F^{\mathrm{cyc}})$ is a torsion module over the Iwasawa algebra $\Lambda(\Gamma)$, where $\Gamma \simeq \mathbb{Z}_p = \mathrm{Gal}(F^{\mathrm{cyc}}/F)$.

The ring $\Lambda(G)$ is known to be a left and right noetherian ring. If G is pro-p and has no elements of order p, it is an Auslander regular, local domain (see [V]). In general however, it is a semilocal ring. The statement of the main conjecture needs the localization sequence, which is contingent on a choice of a left and right Ore set. Recall that $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$.

Definition 3.1. The set S is defined as

$$S = \{x \in \Lambda(G) \mid \Lambda(G)/s\Lambda(G) \text{ is a finitely generated } \Lambda(H) - \text{module}\}.$$

It is proven in [CFKSV] that the set S consists of nonzero divisors and is a left and right Ore set of $\Lambda(G)$. The set S_* is defined by $S_* = \bigcup_{n\geq 0} p^n S$.

In this set-up, we have the localization exact sequence

$$K_1(\Lambda(G)) \to K_1(\Lambda(G)_S) \xrightarrow{\partial} K_0(\Lambda(G), \Lambda(G)_S) \xrightarrow{\eta} K_0(\Lambda(G)) \to K_0(\Lambda(G)_S). \quad (12)$$

It is proven in [FK] that if G is a profinite group, then

$$K_1(\Lambda_{\mathcal{O}}(G)) \simeq \varprojlim K_1(\mathcal{O}[G/U)], \quad (13)$$

where the groups G/U vary over the finite quotients of the profinite group G. An additional important result (see for example [K]) is that the connecting homomorphism ∂ is surjective. This is easily seen to be true when $\Lambda(G)$ is local and G has no element of order p, as then the map η is zero since the last two groups on the right are isomorphic to $\mathbb{Z}$, the isomorphism being given by the rank. The general case needs a little more work, along with the fact that G always contains an open normal pro-p subgroup P. The hypothesis that $\mu = 0$ for the Iwasawa module $X(F^{\mathrm{cyc}})$ guarantees that the module $X(F_\infty)$ is in fact an S-torsion module. However, as we are not assuming that G has no elements of order p, $X(F_\infty)$ might not have a finite resolution by projective modules. We shall therefore associate a complex which we denote by $C(F_\infty/F)$, (see [FK]) with the following properties:

- $H_i(C(F_\infty/F)) = 0$ for $i \neq 0, 1$
- $H_0(C(F_\infty/F)) = \mathbb{Z}_p$ and $H_1(C(F_\infty/F)) = X(F_\infty)$.

Indeed the complex $C(F_\infty/F)$ is defined by $\mathrm{RHom}(\mathrm{R}\Gamma(\mathrm{Gal}(F_\Sigma/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p))$. Moreover, it was proved by Fukaya and Kato [FK] that the complex $C(F_\infty/F)$ is quasi-isomorphic to a bounded complex of finitely generated projective $\Lambda(G)$-modules. It is clear by the remarks above that $\Lambda(G)_S \otimes^L_{\Lambda(G)} C(F_\infty/F)$ is acyclic. Further, there are complexes $C(K/F)$ for any extension $F \subset K \subset F_\infty$ with derived isomorphisms

$$\Lambda(\mathrm{Gal}(K/F)) \otimes^L_{\Lambda(G)} C(F_\infty/F) \simeq C(K/F).$$

Thus there is an object $[C(F_\infty)/F]$ in the category $\mathcal{C}^{hb}_S$ which we then view as being in the relative K-group $K_0(\Lambda(G), \Lambda(G)_S)$ via the isomorphism (7). This object is closely linked to $X(F_\infty)$. In fact, when G has no elements of order p, the module $X(F_\infty)$ can be viewed as an object in the category $\mathcal{H}_S$ and under the isomorphisms in (7), the complex $C(F_\infty/F)$ maps to the module $X(F_\infty)$.

Definition 3.2. Let $\mathcal{O}$ be the ring of integers in a finite extension L of $\mathbb{Q}_p$. If G is a profinite group, then $\mathrm{SK}_1(\Lambda_{\mathcal{O}}(G))$ is defined as the inverse limit

$$\mathrm{SK}_1(\Lambda_{\mathcal{O}}(G)) := \varprojlim \mathrm{SK}_1(\mathcal{O}[G/U])$$

where U varies over open normal subgroups of G and $\mathrm{SK}_1(\mathcal{O}[G/U])$ is defined for the group ring as in (8), noting that G/U is a finite group. The ring $\widehat{\Lambda_{\mathcal{O}}(G)_S}$ is the completion (in the p-adic topology) of the localisation of the Iwasawa algebra $\Lambda_{\mathcal{O}}(G)_S$. We define $\mathrm{SK}_1(\Lambda_{\mathcal{O}}(G)_S)$ and $\mathrm{SK}_1(\widehat{\Lambda_{\mathcal{O}}(G)}_S)$ to be the image of $\mathrm{SK}_1(\Lambda_{\mathcal{O}}(G))$ in $K_1(\Lambda_{\mathcal{O}}(G)_S)$ and in $K_1(\widehat{\Lambda_{\mathcal{O}}(G)_S})$ respectively under the corresponding natural maps

$$K_1(\Lambda_{\mathcal{O}}(G)) \to K_1(\Lambda_{\mathcal{O}}(G)_S) \text{ and } K_1(\Lambda_{\mathcal{O}}(G)) \to K_1(\widehat{\Lambda_{\mathcal{O}}(G)_S}).$$

The following definition extends that of 2.9.

Definition 3.3. Let R denote any of the rings $\Lambda_{\mathcal{O}}(G)$ or $\Lambda_{\mathcal{O}}(G)_S$ or $\widehat{\Lambda_{\mathcal{O}}(G)_S}$. Then we define

$$K_1'(R) = K_1(R)/\mathrm{SK}_1(R).$$

It is easily seen that there is a localization exact sequence

$$K_1(\Lambda(G)) \to K_1'(\Lambda(G)_S) \xrightarrow{\partial} K_0(\Lambda(G), \Lambda(G)_S) \to 0. \tag{14}$$

The formulation of the main conjecture uses this exact sequence along with the fact noted earlier, namely that $[X(F_\infty)]$ lies in the relative K-group $K_0(\Lambda(G), \Lambda(G)_S)$. It is convenient to work with K_1' rather than the K_1 groups in the localization sequence as this gives a uniqueness statement in the main conjecture. To make a precise formulation, we need to discuss noncommutative determinants. Let ρ be a finite dimensional Artin representation of $\mathrm{Gal}(\bar{F}/F)$ factoring through G. Then we have a continuous representation

$$\rho : G \to \mathrm{GL}_n\, \mathcal{O}$$

where $\mathcal{O}$ is the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $Q_{\mathcal{O}}(\Gamma)$ be the fraction field of the Iwasawa algebra $\Lambda_{\mathcal{O}}(\Gamma)$. There is an induced homomorphism (see [CFKSV])

$$\Phi_\rho \, : \, \Lambda(G)_S \to \mathrm{M}_n(Q_{\mathcal{O}}(\Gamma))$$

which by functoriality induces a group homomorphism

$$\Phi'_\rho : K'_1(\Lambda(G)_S) \to K'_1(M_n(Q_{\mathcal{O}}(\Gamma)) = Q_{\mathcal{O}}(\Gamma)^\times,$$

where the last equality holds by Morita invariance. On the other hand, the augmentation map $\phi : \Lambda_{\mathcal{O}}(\Gamma) \to \mathcal{O}$ extends to a homomorphism

$$\phi : \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}} \to L,$$

where $\mathfrak{p}$ is the kernel of ϕ and $\Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}}$ is the corresponding localisation. Extend this map to

$$\phi' : Q_{\mathcal{O}}(\Gamma) \to L \cup \infty$$

by mapping any $x \in Q_{\mathcal{O}}(\Gamma) \setminus \Lambda_{\mathcal{O}}(\Gamma)_{\mathfrak{p}}$ to ∞. Composing Φ'_ρ with ϕ', we get a map

$$\begin{array}{rcl} K'_1(\Lambda(G)_S) & \to & L \cup \infty \\ x & \mapsto & x(\rho). \end{array}$$

Thus elements of $K_1(\Lambda(G)_S)$ can be evaluated on Artin characters to get values. The main conjecture predicts a precise interpolation of these values as below. For any Artin representation ρ of the Galois group of F, let $L_\Sigma(\rho, s)$ denote the imprimitive L-function associated to ρ with the Euler factors at the primes in Σ being removed.

Theorem 3.1 (MAIN CONJECTURE). *Let F_∞/F be an admissible p-adic Lie extension satisfying the hypothesis $\mu = 0$. Then there is a unique element $\zeta(F_\infty/F)$ in $K'_1(\Lambda(G)_S)$ such that $\partial(\zeta(F_\infty/F)) = -[C(F_\infty/F)]$ where $C(F_\infty/F)$ is the complex defined above, and such that for any Artin character ρ of G and any positive integer r divisible by the extension degree $[F_\infty(\mu_p) : F_\infty]$, we have*

$$\zeta(F_\infty/F)(\rho\kappa_F^r) = L_\Sigma(\rho, 1 - r),$$

where κ is the cyclotomic character.

The element $\zeta(F_\infty/F)$ is called a *p-adic zeta function* for the extension F_∞/F. It depends on the finite set Σ but we shall suppress this in the notation. It can be shown that the validity of the Main Conjecture is independent of Σ as long as it contains all the primes of F that ramify in F_∞.

4 Reductions

In this section, we show how the proof of the main conjecture can be reduced to the case when the Galois group G has dimension one, with $G \simeq H \times G_p$, where G_p is a pro-p, p-adic Lie group and H is a finite group. In other words, the validity of the main conjecture for one dimensional p-adic Lie groups implies the main conjecture for p-adic Lie groups of arbitrary dimension. This was first proven by Burns [Bu] using slightly different methods.

We briefly outline the key reduction steps. Needless to say, each stage of the reduction is accompanied by a meticulous book-keeping on the analytic side for the p-adic L-function and a corresponding reduction for the K-groups, on the algebraic side, but we shall suppress a discussion of these aspects in this outline. The reader can check the corresponding precise assertions in the statements of the theorems where the reduction steps are executed. Of course, the "$\mu = 0$" hypothesis, and the admissibility hypothesis for the reduction steps need to be ensured as well, but this is easily checked.

The first reduction is to the case when G is replaced by a quotient G/U where U is an open subgroup of H (here $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$), and normal in G (see Theorem 4.1). We next reduce to the case where G may be replaced by the inverse image in G of a $\mathbb{Q}_p$-elementary subgroup (see Definition 4.2) in a suitable finite quotient G_n under the natural quotient map $G \to G_n$; this is accomplished in Theorem 4.3. The next reduction (cf. Theorem 4.4) is to the case when G may be assumed to be of the form $G \simeq E' \times E \times \Gamma$, where E' is a finite group of order prime to p and E is a finite abelian group. This paves the way via Theorem 4.5 to reduce to the case when G is in fact an $l - \mathbb{Q}_p$-elementary group for a prime $l \neq p$ (cf. Definition 4.3). Theorem 4.6 proves that the main conjecture is true also when G is $p - \mathbb{Q}_p$-elementary. Combining all these results, one then shows that it suffices to prove the main conjecture when $G \simeq \Delta \times G_p$, where Δ is a finite cyclic group of order prime to p, and G_p is a compact p-adic Lie group of dimension one. This is the final assertion which will eventually be proven.

Let us start with some preliminary observations. By a result of Higman (see [O]), it is known that the groups $\mathrm{SK}_1(\mathcal{O}[\Delta])$ are finite for all finite groups Δ. Combining this with (13), for a compact p-adic Lie group P, we have

$$K_1'(\Lambda_{\mathcal{O}}(P)) \simeq \varprojlim_{\Delta} K_1'(\mathcal{O}[\Delta]), \tag{15}$$

where Δ varies over the finite quotients of P. Let G be the Galois group F_∞/F as before. The following set of quotient groups of G plays an important role.

Definition 4.1. The set $Q_1(G) = \{G/U \; : \; U$ is an open subgroup of H and is normal in G$\}$.

Proposition 4.1. *The natural map*

$$K_1'(\Lambda(G)) \to \varprojlim_{G' \in Q_1(G)} K_1'(\Lambda(G'))$$

is an isomorphism.

Proof. We have

$$\begin{aligned}\varprojlim_{G' \in Q_1(G)} K_1'(\Lambda(G')) &\simeq \varprojlim_{G'} \varprojlim_{\Delta_{G'}} K_1'(\mathbb{Z}_p[\Delta_{G'}]) \\ &\simeq \varprojlim_{\Delta} K_1'(\mathbb{Z}_p[\Delta]) \\ &\simeq K_1'(\Lambda(G)),\end{aligned}$$

where $\Delta_{G'}$ runs through finite quotients of G' and Δ runs through all finite quotients of G. □

The first reduction is the following:

Theorem 4.1. *Assume F_∞/F is an admissible p-adic Lie extension satisfying the $\mu = 0$ hypothesis. Then the main conjecture is true for F_∞/F if it is true for each of the extensions F_∞^U/F for all open subgroups $U \subseteq H$ such that U is normal in G, and if for each group $G_U := G/U$, the group $K_1'(\Lambda(G_U))$ injects into $K_1(\Lambda(G_U)_S)$.*

Proof (sketch). Note first that F_∞^U/F is an admissible p-adic Lie extension which again satisfies the $\mu = 0$ Hypothesis. (This is true because the $\mu = 0$ hypothesis is equivalent to $X(F_\infty)$ being finitely generated as a $\Lambda(H)$-module, and observing that $\Lambda(U)$ is a subalgebra of $\Lambda(H)$ with the property that $\Lambda(H)$ is finite as a $\Lambda(U)$-module). Consider now the following commutative diagram:

$$\begin{array}{ccccccccc} & & K_1'(\Lambda(G)) & \longrightarrow & K_1'(\Lambda(G)_S) & \xrightarrow{\partial} & K_0(\Lambda(G), \Lambda(G)_S) & \longrightarrow & 0 \\ & & \wr\downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \varprojlim_{G_U} K_1'(\Lambda(G_U)) & \longrightarrow & \varprojlim_{G_U} K_1'(\Lambda(G_U)_S) & \longrightarrow & \varprojlim_{G_U} K_0(\Lambda(G_U), \Lambda(G_U)_S). & & \end{array}$$

Using the hypothesis on the validity of the main conjecture for the quotients G/U, we see that there exist elements ζ_U in $K_1'(\Lambda(G_U)_S)$ satisfying the main conjecture for each G_U. Let $f \in K_1'(\Lambda(G)_S)$ be a characteristic element of $C(F_\infty/F)$ and let $(f_U)_U \in \varprojlim_{G_U} K_1'(\Lambda(G_U)_S)$ be the image of f under the second vertical map. Put $w_U = \zeta_U f_U^{-1} \in K_1'(\Lambda(G_U)_S)$. Then $(w_U)_{U \in Q_1(G)} \in \varprojlim_{G_U} K_1'(\Lambda(G_U))$. There is an element $w \in K_1'(\Lambda(G))$ that maps to $(w_U)_U$ under the first vertical isomorphism. Let us check that $\zeta := wf$ is the required p-adic zeta function. Uniqueness is clear, and an easy diagram chase gives $\partial(\zeta) = -[C(F_\infty/F)]$.

To check the interpolation property, let ρ be an Artin representation of G. Note first that there is a G' in $Q_1(G)$ such that ρ factors through G'. Since ζ maps to $\zeta_{G'}$ in $K_1(\Lambda(G')_S)$, for any positive integer r divisible by $[F_\infty(\mu_p) : F_\infty]$, we have

$$\zeta(\rho\kappa_F^r) = \zeta_G(\rho\kappa_F^r) = L_\Sigma(\rho, 1 - r),$$

as required. □

The next reduction steps help us to reduce further to special kinds of admissible p-adic extensions of dimension one. Let $\Gamma \simeq \mathbb{Z}_p$ be the Galois group of the cyclotomic extension F^{cyc}/F. Pick and fix a lift of Γ in G so that we get an isomorphism $G \simeq H \rtimes \Gamma$. Fix also an open subgroup Γ^{p^e} of Γ that acts trivially on H and put $G_e = G/\Gamma^{p^e}$. We need the following definitions.

Definition 4.2. Let l be prime integer. A finite group P is called *l-hyperelementary* if P is of the form $C_n \rtimes P_1$, with C_n a cyclic group of order n, l a prime such that $l \nmid n$, and P_1 is a finite l-group. Let K be a field. An l-hyperelementary group $C_n \rtimes P_1$ is called *l-K-elementary* if

$$\mathrm{Im}[P_1 \to \mathrm{Aut}(C_n) \simeq (\mathbb{Z}/n\mathbb{Z})^{\times}] \subset \mathrm{Gal}(K(\mu_n)/K.$$

A *hyperelementary group* is one which is l-hyperelementary for some prime l. A K-elementary group is one which is l-K-elementary for some prime l.

The above definition is extended to p-adic Lie groups as follows.

Definition 4.3. Let l be a prime. A p-adic Lie group is called *l-K-elementary* if it is of the form $P \rtimes \Gamma$ for a finite group P and such that there is a central open subgroup Γ^{p^r} of $P \rtimes \Gamma$ such that $(P \rtimes \Gamma)/\Gamma^{p^r}$ is an l-K-elementary finite group. A p-adic Lie group is K-elementary if it is l-K-elementary for some prime l.

The next tool we use is the induction theory of A. Dress which reduces the computation of K_1' for finite group rings $\mathcal{O}[P]$ to l-K-elementary subgroups of the finite group P, where K is the fraction field of $\mathcal{O}$. In particular, we need the following theorem (see [O, Theorem 11.2] and also [W]).

Theorem 4.2. *Let P be a finite group. Then there is an isomorphism*

$$K_1'(\mathcal{O}[P]) \simeq \varprojlim_{\pi} K_1'(\mathcal{O}[\pi]),$$

where π runs through all K-elementary subgroups of P. The inverse limit is taken with respect to norm maps and the maps induced by conjugation. In other words, $(x_\pi) \in \prod_{\pi} K_1'(\mathcal{O}[\pi])$ lies in $\varprojlim_{\pi} K_1'(\mathcal{O}[\pi])$ if and only if

- *For all $g \in P$, $g x_\pi g^{-1} = x_{g\pi g^{-1}}$, and*
- *For $\pi \leq \pi' \leq P$, the norm homomorphism $K_1'(\mathcal{O}[\pi']) \to K_1'(\mathcal{O}[\pi])$ maps $x_{\pi'} \to x_\pi$.*

Hence in the above isomorphism, we may restrict the inverse limit to only maximal K-elementary subgroups of P.

Lemma 4.1. *Let $G_n = G/\Gamma^{p^{n+e}}$ for all $n \geq 0$. For each n, we have an isomorphism*

$$K_1'(\Lambda(G)) \simeq \varprojlim_{P} K_1'(\Lambda(U_P)),$$

where the inverse limit ranges over all $\mathbb{Q}_p$-elementary subgroups of G_n, and it is with respect to the maps induced by conjugation and the norm maps. The group U_P is the inverse image of P in G under the surjection $G \twoheadrightarrow G_n$.

Proof. Note that G_n is a finite group as we have reduced to the case when G has dimension one. Letting P run through all $\mathbb{Q}_p$-elementary subgroups of G_n and taking all inverse limits with respect to the maps induced by conjugation and the norm maps, by Theorem 4.2 we have an isomorphism

$$K_1'(\mathbb{Z}_p[G_n]) \simeq \varprojlim_{P} K_1'(\mathbb{Z}_p[P])$$

Claim:

$$K_1'(\mathbb{Z}_p[G_{n+i}]) \simeq \varprojlim_{P} K_1'(\mathbb{Z}_p[U_P/\Gamma^{p^{n+e+i}}]).$$

We remark that $U_P/\Gamma^{p^{n+e+i}}$ is the inverse image of P in the group G_{n+i} for all $i \geq 0$, under the surjection $G_{n+i} \to G_n$. Further, any $\mathbb{Q}_p$-elementary subgroup of G_{n+i} is contained in $U_P/\Gamma^{p^{n+e+1}}$ for some P. Hence

$$\begin{aligned}
\varprojlim_{P} K_1'(\mathbb{Z}_p[U_P/\Gamma^{p^{n+e+1}}]) &\simeq \varprojlim_{P}\varprojlim_{C_P} K_1'(\mathbb{Z}_p[C_P]) \\
&\simeq \quad \varprojlim_{Q} K_1'(\mathbb{Z}_p[Q]) \\
&\simeq \quad K_1'(\mathbb{Z}_p[G_{n+i}]);
\end{aligned}$$

where C_P runs through all $\mathbb{Q}_p$-elementary subgroups of $U_P/\Gamma^{p^{n+e+i}}$ and Q runs through all $\mathbb{Q}_p$-elementary subgroups of G_{n+i}. Hence the claim is proved and the lemma follows by passing to the inverse limit and using (15). □

The following theorem reduces proving the main conjecture to the case of $\mathbb{Q}_p$-elementary extensions.

Theorem 4.3. *Assume that the main conjecture is valid for all one dimensional, admissible p-adic Lie extensions satisfying $\mu = 0$ hypothesis and whose Galois group is $\mathbb{Q}_p$-elementary. Also assume that for all $\mathbb{Q}_p$-elementary p-adic Lie groups U, the group $K_1'(\Lambda(U))$ injects into $K_1'(\Lambda(U)_S)$. Then the main conjecture is valid for all admissible p-adic Lie extensions F_∞/F satisfying $\mu = 0$ hypothesis. Moreover, if $G = \mathrm{Gal}(F_\infty/F)$, then $K_1'(\Lambda(G))$ injects into $K_1'(\Lambda(G)_S)$.*

Proof. We sketch the essential steps. First note that if the $\mu = 0$ hypothesis is valid for an admissible p-adic Lie extension F_∞/F of dimension one, then it is valid for all its admissible p-adic Lie subextensions as well. This is a consequence of the fact that $\mu = 0$ is equivalent to $X(F_\infty)$ being a finitely generated module over $\mathbb{Z}_p[H]$ where $H = \mathrm{Gal}(F_\infty/F^{\mathrm{cyc}})$. Assume that the main conjecture is valid for all admissible p-adic Lie subextensions of F_∞/F whose Galois group is $\mathbb{Q}_p$-elementary, and let $G_n = G/\Gamma^{p^{n+e}}$, for $n \geq 0$. Consider the following commutative diagram where P runs through all $\mathbb{Q}_p$-elementary subgroups of G_n and U_P denotes the inverse image of P in G.

$$\begin{array}{ccccccccc} & & K_1'(\Lambda(G)) & \longrightarrow & K_1'(\Lambda(G)_S) & \xrightarrow{\partial} & K_0(\Lambda(G),\Lambda(G)_S) & \longrightarrow & 0 \\ & & \wr\downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \varprojlim_P K_1'(\Lambda(U_P)) & \longrightarrow & \varprojlim_P K_1'(\Lambda(U_P)_S) & \longrightarrow & \varprojlim_P K_0(\Lambda(U_P),\Lambda(U_P)_S). & & \end{array}$$

Pick f in $K_1'(\Lambda(G)_S)$ such that $\partial(f) = -[C(F_\infty)/F]$ and let (f_P) be its image in $\varprojlim_P K_1'(\Lambda(U_P)_S)$. From our hypothesis, we get a p-adic zeta function ζ_P for each P, which gives, by uniqueness, an element $(\zeta_P) \in \varprojlim_P K_1'(\Lambda(U_P)_S)$. Put $u_P = \zeta_P f_P^{-1} \in K_1'(\Lambda(U_P))$ and note that there is a $u \in K_1'(\Lambda(G))$ mapping to (u_P). Then $\zeta = uf$ is the sought after p-adic L-function. Being the only element in $K_1'(\Lambda(G)_S)$ such that $\partial(\zeta) = -[C(F_\infty/F)]$ and whose image in $K_1'(\Lambda(U_P))$ is ζ_P, it is independent of the choice of n.

The interpolation property is seen to hold as follows. Let ρ be an Artin character of G, then ρ factors through a quotient G_n for some n. By the Brauer Induction theorem (see [CR, (15.9)]), we can write

$$\rho = \sum_P n_p \operatorname{Ind}_{U_P}^G \rho_P,$$

remembering that P runs through $\mathbb{Q}_p$-elementary subgroups of G_n, and also that ρ_P's need not be one dimensional. Let F_P denote the field extension of F that is the fixed field of U_P and suppose that κ_{F_P} is the corresponding cyclotomic character. For any positive integer r divisible by $[F_\infty(\mu_p) : F_\infty]$, we then have

$$\begin{aligned} \zeta(\rho\kappa_F^r) &= \prod_P \zeta(\operatorname{Ind}_{U_P}^G \rho_P \kappa_F^r)^{n_\rho} \\ &= \prod_P \zeta_P(\rho_P \kappa_{F_P}^r)^{n_P} \\ &= \prod_P L_\Sigma(\rho_P, 1-r)^{n_P}, \end{aligned}$$

thereby establishing the interpolation property. The remaining assertion follows easily from a diagram chase and the theorem is proved. □

We have thus reduced the proof of the main conjecture to $\mathbb{Q}_p$-elementary extensions. Within this reduction, we proceed to analyse the case under the assumption that G is $l-\mathbb{Q}_p$-elementary for some prime $l \neq p$. The first observation is the following

Lemma 4.2. *If a p-adic Lie group G is l-$\mathbb{Q}_p$-elementary for some prime $l \neq p$, then it is isomorphic to $\Gamma^{p^e} \times E$ for some finite l-$\mathbb{Q}_p$-elementary group E.*

Proof. Write $G = H \rtimes \Gamma$. Let Γ^{p^r} be a central open subgroup of G such that G/Γ^{p^r} is $l - \mathbb{Q}_p$-elementary. Choose $e \geq 0$ to be the smallest integer such that Γ^{p^e} is an open central subgroup of G. Then $G' := G/\Gamma^{p^e}$ is an $l - \mathbb{Q}_p$-elementary finite group. We prove that $G = \Gamma^{p^e} \times G'$. Write $G' = C \rtimes P$, where C is a cyclic subgroup of G of order prime to l and P is an l-group. We have $C \rtimes P = G' = H \rtimes \Gamma/\Gamma^{p^e}$. The order of P being prime to p, it is a subgroup of H and is hence also a subgroup of G. Let U_C be the inverse image of C in G. As Γ^{p^e} is central and C is cyclic, U_C is an abelian group. We write $U_C = Q \times D$, where Q is a pro-p, pro-cyclic subgroup of U_C and D is a torsion subgroup. Then $G = (Q \times D) \rtimes P$. The action of P on Q is necessarily trivial, as it is trivial on an open subgroup of Q. Hence Q is a central pro-cyclic subgroup of G whence $Q = \Gamma^{p^e}$ and $D = C$. This completes the proof. □

This lemma enables us to take the further step of reducing to the case when G is of the form $\Gamma \times E$, with E an l-$\mathbb{Q}_p$-elementary finite group. We may write $E = C \rtimes U$ where C is a cyclic group of order prime to l and U is a finite l-group. If $p \nmid$ the order of C, then the main conjecture is valid for F_∞/F by the following classical theorem (see [CK]).

Theorem 4.4. *Let F_∞/F be a p-adic Lie extension with Galois group $G = E' \times E \times \Gamma$ where E' is a finite group whose order is prime to p and E is a finite abelian group. Then the main conjecture is true for the extension F_∞/F.* □

The main idea in the proof of the above theorem is to use the images C_χ of the complex $C(F_\infty/F)$ for characters χ in the set $R(\chi)$ of irreducible characters of E', where

$$C_\chi := (\Lambda_{\mathcal{O}_\chi}(E \times \Gamma))_S \otimes^L_{\Lambda(G)_S} C(F_\infty/F).$$

Then

$$\partial(L_p(\chi)) = -[C_\chi] \in K_0(\Lambda_{\mathcal{O}_\chi}(E \times \Gamma), \Lambda_{\mathcal{O}_\chi}(E \times \Gamma)_S).$$

One then uses the isomorphism

$$K_0(\Lambda(G), \Lambda(G)_S) \to \bigoplus_{\chi \in R(E')} K_0(\Lambda_{\mathcal{O}_\chi}(E \times \Gamma), \Lambda_{\mathcal{O}_\chi}(E \times \Gamma)_S).$$

Thus if p divides the order of the cyclic group C, working with the Sylow subgroups of C, we may split the semidirect product and assume that our group G is an l-$\mathbb{Q}_p$-elementary group of the form

$$G = \Gamma \times H \text{ with } H = C \rtimes P, \tag{16}$$

with C a cyclic group of p-power order and P a finite group of order prime to p. By a result of Oliver (see [O, Proposition 12.7]), if G' is a finite group such that the p-Sylow subgroup of G' has an abelian normal subgroup with cyclic quotient, then $SK_1(\mathbb{Z}_p[G']) = 1$. By passing to the inverse limit, one then concludes that $SK_1(\mathbb{Z}_p[G]) = 1$ for G as reduced above in (16).

Definition 4.4. Let G be as in (16). Since P acts on C, the homology groups $H_i(P, C)$ are defined. Put $\bar{C} = H_0(P, C)$, $\bar{H} = \bar{C} \times P$ and $\bar{G} = \Gamma \times \bar{H}$. Define $P_1 = \mathrm{Ker}\,(P \to \mathrm{Aut}(C))$, $H_1 = C \times P_1$, and $G_1 = \Gamma \times H_1$.

We have the natural maps

$$norm : K_1(\Lambda(G)) \to K_1(\Lambda(G_1)).$$

$$\begin{aligned} \theta : K_1(\Lambda(G)) &\to K_1(\Lambda(\bar{G})) \times K_1(\Lambda(G_1)), \\ \theta_S : K_1(\Lambda(G)_S) &\to K_1(\Lambda(\bar{G})_S) \times K_1(\Lambda(G_1)_S), \end{aligned} \tag{17}$$

where the map in the first component is the one induced by the natural surjection and the map in the second component is the norm map. This is used to define the following set which will play a key role in the description of $K_1(\Lambda(G))$.

Definition 4.5. Consider the maps

$$can : K_1(\Lambda(G_1)) \to K_1(\Lambda(\Gamma \times \bar{C})), \quad norm : K_1(\Lambda(\bar{G})) \to K_1(\Lambda(\Gamma \times \bar{C})).$$

Let Φ (resp. Φ_S) be the group whose underlying set consists of all pairs $(x_0, x_1) \in K_1(\Lambda(\bar{G}) \times K_1(\Lambda(G_1))$ (resp. $K_1(\Lambda(\bar{G})_S) \times K_1(\Lambda(G_1)_S))$) such that $norm(x_0) = can(x_1)$, and x_1 is fixed under the conjugation action by every element of P.

Proposition 4.2. *The map θ induces an isomorphism between $K_1'(\Lambda(G))$ and Φ. The image of θ_S is contained in Φ_S. In particular*

$$\mathrm{Im}(\theta_S) \cap (K_1(\Lambda(\bar{G})) \times K_1(\Lambda(G_1))) = \mathrm{Im}(\theta).$$

Thus there is a commutative diagram

$$\begin{array}{ccc} K_1(\Lambda(G)) & \xrightarrow{\theta} & \Phi \subseteq K_1(\Lambda(\bar{G})) \times K_1(\Lambda(G_1)) \\ \downarrow & & \downarrow \\ K_1(\Lambda(G)_S) & \xrightarrow{\theta_S} & \Phi_S \subseteq K_1(\Lambda((\bar{G}))_S) \times K_1(\Lambda(G_1)_S). \end{array}$$

Proof. Let us verify that the image of θ is contained in Φ; the corresponding verification for θ_S is similar. Let B be the set of right coset representatives of C in H. Then B is a basis of the $\Lambda(G_1)$-module $\Lambda(G)$. Let $x \in K_1(\Lambda(G))$. The image of x in $K_1(\Lambda(G_1))$ under the norm map is described as follows. Let $\tilde{x}$ be a lift of x in $\Lambda(G)^\times$. Multiplication on the right by $\tilde{x}$ gives a $\Lambda(G_1)$-linear map on $\Lambda(G)$. Let $A(B, \tilde{x})$ be the matrix of this map with respect to the basis B. Then the norm of x is the class of this matrix in $K_1(\Lambda(G_1))$, and is independent of $\tilde{x}$ and the basis B.

Let $g \in P$. Then gBg^{-1} is also a $\Lambda(G_1)$-basis of $\Lambda(G)$, and we have $gA(B, \tilde{x})g^{-1} = A(gBg^{-1}, g\tilde{x}g^{-1})$. Since $g\tilde{x}g^{-1}$ is also a lift of x, the class of $A(gBg^{-1}, g\tilde{x}g^{-1})$ in $K_1(\Lambda(G_1))$ is the same as that of $A(B, \tilde{x})$. Hence $\theta(x)$ satisfies the second condition on the definition of Φ, namely invariance under conjugation. Choosing the same set B as a basis of the $\Lambda(\Gamma \times \bar{C})$-module $\Lambda(\bar{G})$, one sees that the following diagram commutes:

$$\begin{tikzcd} K_1(\Lambda(G)) \arrow[r, "norm"] \arrow[d, "can"'] & K_1(\Lambda(G_1)) \arrow[d, "can"] \\ K_1(\Lambda(\bar{G})) \arrow[r, "norm"'] & K_1(\Lambda(\Gamma \times \bar{C})). \end{tikzcd}$$

Hence $\theta(x)$ also satisfies the first condition in the definition of Φ.

We show that θ surjects onto Φ. Let $(x_0, x_1) \in \Phi$. Since $K_1(\Lambda(G))$ surjects onto $K_1(\Lambda(\bar{G}))$, we can assume that $x_0 = 1$. Then the first condition in the definition of Φ implies that

$$x_1 \in J := \mathrm{Ker}\,(can : K_1(\Lambda(G_1)) \to K_1(\Lambda(\Gamma \times \bar{C}))).$$

By Oliver [O, Theorem 2.10] and Fukaya and Kato [FK, Proposition 1.5.3], the subgroup J is pro-p. Let J^P be the subgroup of elements of J that are fixed pointwise under the conjugation action of P. Note that the above result tells us that J^P is pro-p as well. Let $x_1 \in J^P$, and suppose that n is the order of P. Let $z \in J^P$ be such that $z^n = x_1$. Denote by z the image of z in $K_1(\Lambda(G))$. Let $\theta(z) = (z_0, z_1)$. By construction, we have $z_1 = x_1$, and we have $norm(z_0) = z_0^n = 1$ in $K_1(\Lambda(\Gamma \times \bar{C}))$. But z_0 lies in a pro-p subgroup and hence $z_0 = 1$, thereby proving the surjectivity of θ onto Φ.

We now show that θ is injective. For a finite group G', let $Conj(G')$ denote the set of conjugacy classes of G'. Let n be a non-negative integer. Consider the map

$$\beta : \mathbb{Q}_p[Conj(G/\Gamma^{p^n})] \to \mathbb{Q}_p[Conj(\bar{G}/\Gamma^{p^n})] \times \mathbb{Q}_p[G_1/\Gamma^{p^n}]$$

where the map into the first component is induced by the natural surjection and the map into the second component is defined as follows. Let B be a set of left coset representatives of C in G/Γ^{p^n} and let $g \in G/\Gamma^{p^n}$. Then the map is the $\mathbb{Q}_p$-linear map induced by

$$g \mapsto \sum_{x \in B} \{x^{-1}gx : x^{-1}gx \in G_1/\Gamma^{p^n}\}.$$

To see this injectivity, we need to use some representation theory. Recall that H is isomorphic to $C \rtimes P$ with C a cyclic group of order a power of p which is prime to l and P a finite l-group. If $\hat{C}$ denotes the set of irreducible characters of C, then P acts on $\hat{C}$ by $(g.\chi)(h) = \chi(ghg^{-1})$, for $g \in P$, $\chi \in \hat{C}$ and $h \in C$. Under this action by P, the stabilizer of χ is P_1 if $\chi \neq 1$. Indeed, let $\chi \in \hat{C}$ and $\chi \neq 1$.

If $g.\chi = \chi$, then $\chi(ghg^{-1}) = \chi(h)$ for all $h \in C$ and hence the commutator $ghg^{-1}h^{-1} \in \text{Ker } \chi$ for all $h \in C$. In particular, if c is a generator of C, then as $\chi \neq 1$, Ker χ is a proper subgroup of C. Thus if $gcg^{-1} = c^a$, then $a \equiv 1 \bmod p$. But the order of P is prime to p and hence $a^{p-1} \equiv 1 \bmod \mid C \mid$. Hence $a \equiv 1$ modulo $\mid C \mid$ and $g \in P_1$. For a system of representatives $\{\xi_i\}$ of orbits of this action of P on $\hat{C}$, let P_i denote the stabilizer of ξ_i. By Serre [Se, Proposition 25] (see also [CR, Theorem 11.11]), we deduce that every irreducible representation of H is obtained by inducing an irreducible representation of $C \rtimes P_i$, which in turn is obtained by taking an irreducible representation of P_i, inflating it to $C \rtimes P_i$, and twisting it by ξ_i. We have just argued that P_i is either P (when the character is trivial) or is equal to P_1. Noting that no nontrivial character of C is fixed by this action of P, the latter case reduces to inflating from P, which does give a smaller set of representations than those inflated from $\bar{C} \times P$, we obtain the following lemma.

Lemma 4.3. *Any irreducible representation of H is obtained either by inflating an irreducible representation of $\bar{C} \times P$ or by inducing an irreducible representation of H_1.* $\square$

For a finite group K, let $R(K)$ be the ring of virtual characters of K. The map

$$\begin{array}{ccc} \bar{\mathbb{Q}}_p \otimes_{\mathbb{Z}} R(\bar{G}/\Gamma^{p^n}) \times \bar{\mathbb{Q}}_p \otimes_{\mathbf{Z}} R(G_1/\Gamma^{p^n}) & \to & \bar{\mathbb{Q}}_p \otimes_{\mathbb{Z}} R(G/\Gamma^{p^n}) \\ (\chi, \rho) & \mapsto & \mathrm{Inf}(\chi) + \mathrm{Ind}(\rho), \end{array}$$

where Inf denotes the inflating homomorphism and Ind is the induced representation, is surjective by Lemma 4.3. Clearly, $\mathrm{Id}_{\bar{\mathbb{Q}}_p} \otimes \beta$ is dual to the above map described in Lemma 4.3. It follows therefore that β is injective. It induces an injection

$$\beta \, : \, \varprojlim_n \mathbb{Q}_p[Conj(G/\Gamma^{p^n}] \to \varprojlim_n \mathbb{Q}_p[Conj(\bar{G}/\Gamma^{p^n}] \times \varprojlim_n \mathbb{Q}_p[G_1/\Gamma^{p^n}].$$

A final crucial ingredient in proving the injectivity of θ is the *logarithm* map on K_1 (see [SV]) defined by Oliver and Taylor. For a finite group G', there is a group homomorphism

$$log \, : \, K_1(\mathbb{Z}_p[G']) \to \mathbb{Q}_p[Conj(G)]$$

with kernel the torsion subgroup. By a result of Wall [W, Proposition 6.5], the torsion subgroup of $K_1(\mathbb{Z}_p[G'])$ is $\mu_{p-1} \times G^{\mathrm{ab}} \times SK_1(\mathbb{Z}_p[G])$. Thus the exact sequence

$$1 \to \mu_{p-1} \times (G/\Gamma^{p^n})^{\mathrm{ab}} \to K_1(\mathbb{Z}_p[G/\Gamma^{p^n}]) \xrightarrow{log} \mathbb{Q}_p[Conj(G/\Gamma^{p^n})]$$

induces a homomorphism

$$1 \to \mu_{p-1} \times G^{\mathrm{ab}} \to K_1(\Lambda(G)) \xrightarrow{log} \varprojlim_n \mathbb{Q}_p[Conj(G/\Gamma^{p^n})].$$

There is a commutative diagram (see proof of [O, Theorem 6.8])

$$\begin{tikzcd} K_1(\Lambda(G)) \arrow[r, "log"'] \arrow[d, "\theta"'] & \varprojlim_n \mathbb{Q}_p[Conj(G/\Gamma^{p^n})] \arrow[d, "\beta"] \\ K_1(\Lambda(\bar{G})) \times K_1(\Lambda(G_1)) \arrow[r, "log"] & \varprojlim_n \mathbb{Q}_p[Conj(\bar{G}/\Gamma^{p^n})] \times \varprojlim_n \mathbb{Q}_p[G_1/\Gamma^{p^n}]. \end{tikzcd}$$

We complete the proof of the injectivity of θ. Let $x \in Ker(\theta)$. As β is injective, $x \in \mathrm{Ker}\,(log)$, and hence $x \in \mu_{p-1} \times G^{\mathrm{ab}}$. But under the natural surjection

$$K_1(\Lambda(G)) \to K_1(\Lambda(\bar{G})),$$

which is in fact the first component of the map θ, $\mu_{p-1} \times G^{\mathrm{ab}}$ maps identically on $\mu_{p-1} \times (\bar{G})^{ab}$ (note that $G^{\mathrm{ab}} = \bar{G}^{\mathrm{ab}}$). Hence $x = 1$ and the proposition is proved. □

Theorem 4.5. *Let F_∞/F be an admissible extension satisfying the hypothesis $\mu = 0$ and let $G = \mathrm{Gal}(F_\infty/F)$. Assume that G is $l - \mathbb{Q}_p$-elementary for some prime $l \neq p$. Then the main conjecture for F_∞/F is valid. Moreover, $K_1(\Lambda(G))$ injects into $K_1(\Lambda(G)_S)$.*

Proof. Let $f \in K_1(\Lambda(G)_S)$ such that $\partial(f) = -[C(F_\infty/F)]$, and let $\theta_S(f) = (f_0, f_1) \in \Phi_S$. Recall that $G_1 \simeq \Gamma \times C$ with C a cyclic group of p-power order, and $\bar{G} \simeq \Gamma \times \bar{C} \times P$, with P a finite group of order prime to p. Let $L = F_\infty^{G_1}$, and F'_∞/F be the Galois extension of F such that $\mathrm{Gal}(F'_\infty/F) = \bar{G}$. By the earlier reductions, the main conjecture is valid for subextensions F_∞/L and the extension F'_∞/F. Let ζ_1 and ζ_0 be the corresponding p-adic zeta functions satisfying the main conjecture. By the uniqueness and the interpolation property, one verifies that $(\zeta_0, \zeta_1) \in \Phi_S$. Let $u_i = \zeta_i f_i^{-1}$ (for $i = 0, 1$). Then $(u_0, u_1) \in \Phi$, and we pick $u \in K_1(\Lambda(G))$ be the unique element such that $\theta(u) = (u_0, u_1)$. Now $\zeta = uf$ is the required p-adic ζ-function. That $\partial(f) = -[C(F_\infty)/F]$ is clear, and we check the interpolation property. By Lemma 4.3, ρ is either obtained by inflating a representation $\bar{\rho}$ of $\bar{G}$ or by inducing a representation ρ_1 of G_1. Hence for any positive integer r divisible by $[F_\infty(\mu_p) : F_\infty]$, we have for $i = 0$ or 1, and $\kappa_0 = \kappa_F, \kappa_1 = \kappa_L$,

$$\zeta(\rho\kappa_F^r) = \zeta_i(\rho_i\kappa_i^r) = L_\Sigma(\rho_i, 1-r) = L_\Sigma(\rho, 1-r).$$

To see the assertion about injectivity, note that if $x \in K_1(\Lambda(G))$ maps to 1 in $K_1(\Lambda(G)_S)$, then $\theta(x) = 1$ and hence $x = 1$. Hence the theorem is proved. □

The final reduction is to pro-p extensions. We may assume by the results proved so far that G/Γ^{p^e} is p-$\mathbb{Q}_p$-elementary, say $G/\Gamma^{p^e} = C_n \rtimes H_p$ where H_p is a p-group and C_n is a cyclic group of order n prime to p. The Galois group $\mathrm{Gal}(\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p)$ acts on the set of one dimensional characters $\hat{C}_n$ of C_n, and we let C be the orbit set of $\hat{C}_n$ under this action. Then the ring $\mathbb{Z}_p[C_n]$ decomposes as

$$\mathbb{Z}_p[C_n] \simeq \bigoplus_{\chi} \mathcal{O}_\chi,$$

where χ varies over a representative character from each orbit, and $\mathcal{O}_\chi$ is the ring of integers in a finite extension L_χ of $\mathbb{Q}_p$. The action of H_p on C_n induces an action on each $\mathcal{O}_\chi$ through

$$H_p \to \mathrm{Gal}(L_\chi/\mathbb{Q}_p).$$

Set U_{H_p} to be the inverse image of H_p in G which for ease of notation, we denote by U. Then $G = C_n \rtimes U$. Let t_χ denote the composition

$$t_\chi \,:\, U \to H_p \to \mathrm{Gal}(L_\chi/\mathbb{Q}_p),$$

and let U_χ denote Ker (t_χ).

Proposition 4.3. *We have an isomorphism*

$$K_1'(\Lambda(G)) \to \bigoplus_{\chi} K_1'(\Lambda_{\mathcal{O}_\chi}(U_i))^{U/U_\chi}.$$

Proof. For every $n \geq 0$, let $G_n = G/\Gamma^{p^{n+e}}$. Define $U_{\chi,n}$ to be the kernel of the composite map

$$U/\Gamma^{p^{e+n}} \to H_p \to \mathrm{Gal}(L_\chi/\mathbb{Q}_p).$$

Then by Oliver [O, Theorem 12.3], we have

$$K_1'(\mathbb{Z}_p[G_n]) \simeq \bigoplus_{\chi} K_1'(\mathcal{O}_\chi[U_{\chi,n}])^{U/U_{\chi,n}}.$$

The required result follows on passing to the inverse limit. □

Let us recall the set-up; we have now reduced to the case where $G = \mathrm{Gal}(F_\infty/F)$ is a p-adic Lie extension such that it satisfies the $\mu = 0$ hypothesis and such that G is a p-$\mathbb{Q}_p$-elementary subgroup which contains a fixed open subgroup Γ^{p^e} of Γ which is central in G. Let χ be a character as in the paragraph above.

Theorem 4.6. *Let F_∞/F be a p-adic Lie extension satisfying $\mu = 0$ hypothesis such that G is a p-$\mathbb{Q}_p$-elementary group $G = C_n \rtimes U_\chi$. With notation as above, assume that the main conjecture is true for $F_\infty^{\mathrm{Ker}\,\chi}/F_\infty^{C_n \rtimes U_\chi}$ for each $\chi \in \hat{C}_n$ and that $K_1'(\Lambda_{\mathcal{O}_\chi}(U_\chi))$ injects into $K_1'(\Lambda_{\mathcal{O}_\chi}(U_\chi)_S)$. Then the main conjecture is true for F_∞/F and $K_1'(\Lambda(G))$ injects into $K_1'(\Lambda(G)_S)$.*

Proof. Assume that the main conjecture is valid for each of the extensions $F_\infty^{\mathrm{Ker}\,\chi}/F_\infty^{C_n \rtimes U_\chi}$. Let $\zeta_\chi \in K_1'(\Lambda((C_n/(\mathrm{Ker}\,\chi) \times U_\chi)_S))$ be the p-adic zeta function in the main conjecture. Let $L_p(\chi)$ be the image of ζ_χ under the natural map

$$K_1'(\Lambda((C_n/\mathrm{Ker}\,\chi) \times U_\chi)_S) \to K_1'(\Lambda_{\mathcal{O}_\chi}(U_\chi)_S),$$

induced by the natural surjection $\mathbb{Z}_p[C_n/\mathrm{Ker}\ \chi] \to \mathcal{O}_\chi$. Consider the following commutative diagram

$$\begin{array}{ccccc} K_1'(\Lambda(G)) & \longrightarrow & K_1'(\Lambda(G)_S) & \xrightarrow{\partial} & K_0(\Lambda(G), \Lambda(G)_S) \\ \wr\downarrow & & \downarrow & & \downarrow \\ \bigoplus_\chi K_1'(\Lambda_{\mathcal{O}_\chi}(U_\chi))^{U/U_\chi} & \longrightarrow & \bigoplus_\chi K_1'(\Lambda_{\mathcal{O}_\chi}(U_\chi)_S)^{U/U_\chi} & \xrightarrow{\partial} & K_0(\Lambda_{\mathcal{O}_\chi}(U_\chi), \Lambda_{\mathcal{O}_\chi}(U_\chi)_S). \end{array}$$

We have $L_p(\chi) \in K_1'(\Lambda_{\mathcal{O}_\chi}(U_\chi))^{U/U_\chi}$. Suppose $f \in K_1'(\Lambda(G)_S)$ is such that $\partial(f) = -[C(F_\infty/F)]$. Denote the image of f under the middle vertical arrow by (f_χ), and put $u_\chi = L_p(\chi) f_\chi^{-1}$. Then $(u_\chi) \in \bigoplus_\chi K_1'(\Lambda_{\mathcal{O}_\chi}(U_\chi))^{U/U_\chi}$, and there is a unique u in $K_1(\Lambda(G))$ mapping to (u_χ) under the left vertical isomorphism. Then $\zeta := uf$ is the sought after p-adic L-function. We only check the interpolation property. Let ρ be an irreducible Artin representation of G. Then by Serre [Se, Proposition 25], there is a χ and an Artin representation ρ_χ of U_χ such that

$$\rho = \mathrm{Ind}_{C_n \rtimes U_\chi}^G (\chi \rho_\chi).$$

Thus for any positive integer r divisible by $[F_\infty(\mu_p) : F_\infty]$, we get

$$\zeta(\rho \kappa_F^r) = \zeta_\chi(\chi \rho_\chi \kappa^r) = L_\Sigma(\rho, 1-r),$$

where κ is the p-adic cyclotomic character of $F_\infty^{C_n \rtimes U_\chi}$. The uniqueness of the p-adic zeta function and the statement about K_1'-groups follows from an easy diagram chase and the theorem is proved. □

We have thus reduced the proof of the main conjecture to the case where the Galois group G is of the form $G = \Delta \times G_p$, where Δ is a finite cyclic group of order prime to p and G_p is a pro-p compact p-adic Lie group of dimension 1. This completes the reduction we set out to make and the algebraic aspects of the study of $K_1(\Lambda(G))$ for such groups G will be discussed in the article [SV].

References

[B] H. Bass, *Algebraic K-Theory* (W. A. Benjamin, Inc., New York/Amsterdam, 1968)

[Bj] J.-E. Björk, Filtered Noetherian rings, in *Noetherian Rings and Their Applications (Oberwolfach, 1983), 5997*. Mathematical Surveys and Monographs, vol. 24 (American Mathematical Society, Providence, 1987)

[Bu] D. Burns, On main conjectures in noncommutative Iwasawa theory and related conjectures, preprint (2010) http://www.mth.kcl.ac.uk/staff/dj_burns/newdbpublist.html

[CK] J. Coates, D. Kim, Introduction to the work of M. Kakde on the non-commutative main conjectures for totally real fields, This volume

[CFKSV] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, The GL_2 main conjecture for elliptic curves without complex multiplication. Publ. Math. IHES **101**, 163–208 (2005)

[CR] C. Curtis, I. Reiner, *Methods of Representation Theory with applications to Finite Groups and Orders* (Wiley, New York, 1981)

[FK] T. Fukaya, K. Kato, A formulation of conjectures on p-adic zeta functions in noncommutative Iwasawa theory, in *Proceedings of the St. Petersburg Mathematical Society*, vol. 12, ed. by N.N. Uraltseva (American Mathematical Society, Providence, 2006), pp. 1–85

[K] M. Kakde, The Main Conjecture of Iwasawa theory for totally real fields, preprint (2011)

[Mi] J. Milnor, *Introduction to Algebraic K-Theory*. Annals of Mathematics Studies (Princeton University Press, Princeton, 1971)

[O] R. Oliver, *Whitehead Groups of Finite Groups*. London Mathematical Society Lecture Note Series, vol. 132 (Cambridge University Press, Cambridge/New York, 1988)

[RW] J. Ritter, A. Weiss, On the 'main conjecture' of equivariant Iwasawa theory. J. Am. Math. Soc. **24**, 1015–1050 (2011)

[SV] P. Schneider, O. Venjakob, K_1 of certain Iwasawa algebras, after Kakde, This volume

[Se] J.-P. Serre, *Linear Representation of Finite groups*. Graduate Texts in Mathematics (Springer, New York, 1977)

[Sw] R. G. Swan, *Algebraic K-Theory*. Lecture Notes in Mathematics, vol. 76 (Springer, Berlin/New York, 1968)

[V] O. Venjakob, On the structure theory of the Iwasawa algebra of a p-adic Lie group. J. Eur. Math. Soc. **4**, 271–311 (2002)

[V1] O. Venjakob, On the work of Ritter and Weiss in comparison with Kakde's approach, This volume

[W] C.T.C. Wall, Norms of units in group rings. Proc. Lond. Math. Soc. **29**, 593–632 (1974)

[We] C. Weibel, The K-book: an introduction to algebraic K-theory, Available at http://www.math.rutgers.edu/~weibel/Kbook.html

[Wi] A. Wiles, The Iwasawa conjecture for totally real fields. Ann. Math. **131**, 493–540 (1990)

http://www.springer.com/978-3-642-32198-6

Noncommutative Iwasawa Main Conjectures over Totally Real Fields
Münster, April 2011
Coates, J.; Schneider, P.; Ramdorai, S.; Venjakob, O. (Eds.)
2013, XII, 208 p., Hardcover
ISBN: 978-3-642-32198-6